## REMARKS

Claims 1-20 are currently pending in the subject application and are presently under consideration. Claims 1, 4, 8, 13 and 17-20 have been amended as shown at pp. 2-8 of the Reply.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

### I. Rejection of Claims 1, 3-4, 7 and 19-20 Under 35 U.S.C. §103(a)

In the Final Office Action dated July 5, 2006, claims 1, 3-4, 7 and 19-20 stand rejected under 35 U.S.C. §103(a) as being un-patentable over Sheldon *et al.* (US Patent App. No. 2003/0081125) in view of Flowers *et al.* (US Patent 6,957,348). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Sheldon *et al.* and Flowers *et al.*, individually or in combination, do not teach or suggest each and every element as set forth in the subject claims.

> To reject claims in an application under §103, an examiner must show an unrebutted *prima facie* case of obviousness. A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *See* MPEP §706.02(j). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicants' disclosure. *See In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The claimed invention relates to a system and methodology to facilitate network diagnostics and self-healing of network connectivity problem(s). More particularly, independent claim 1 (and similarly independent claims 4, 19 and 20) recites a protocol diagnostic system, comprising *a data stream monitor component...; and a diagnostics engine comprising at least one protocol state compressor..., and the data stream monitor component utilizes at least one lexical rule set associated with the at least one protocol state compressor to determine subsets of the raw network data to copy, the at least one lexical rule set stores at least one of information regarding structure of subsets of data and protocol specific information; and where* ***the diagnostic engine, upon initialization, stores information associated with protocols to be monitored in the at least one lexical rule set, upon occurrence of a network connectivity problem, stores information associated with additional***

***protocols, and upon correction of the network problem, deletes information associated with selected protocols from the at least one lexical rule set.*** Sheldon *et al.* and Flowers *et al.* do not expressly or inherently disclose the aforementioned novel aspects of applicants' invention as recited in the subject claims.

Sheldon *et al.* discloses a system and method for monitoring and diagnosis of video device performance in the transferring of audio visual data over a video network. A diagnostic node interfaces with a video network to receive audio visual data associated with one or more video devices of the video network. The diagnostic node operates as a transparent pass through/proxy for a video device or as a regular terminating route in order to evaluate audio visual data and determine performance statistics associated with a predetermined video device that is proximate the diagnostic node. (*See* page 1, paragraph [0008]).

Sheldon *et al.* does not disclose the use of a lexical rule set for determining subsets of the raw network data to copy. The lexical rule set can store information regarding structure of subsets of data (*e.g.,* frames) the diagnostics engine desires the data stream monitor component to copy and provide to the protocol state compressors. The lexical rule set can also provide structural information to the data stream monitor component regarding protocols to be monitored. Accordingly, utilizing the lexical rule set, the data stream monitor component can determine which subsets of raw network data to copy and/or an amount of the raw network data to copy. For example, the lexical rule set associated with a particular protocol (*e.g.,* HTTP) can specify that only a portion of a data frame associated with the protocol be copied (*e.g.,* header information). (See pg. 7, line 5-pg. 8, line 20). In contrast, Sheldon *et al.* discloses a diagnostic node deployed as an II.323 protocol compliant terminating route or an H.323 protocol compliant pass through proxy so that audio visual data passed through the network is available to the diagnostic node without interfering with any on-going video calls. (*See* pg. 2, paragraph [0018]). Accordingly, Sheldon *et al.* is silent with regard to ***the use of a lexical rule set to determine subsets of raw network data to copy, wherein the lexical rule set stores information regarding structure of subsets of data and protocol specific information***.

Flowers *et al.* does not cure the deficiencies of Sheldon *et al.* with respect to claims 1, 4, 19 and 20 (which claims 3 and 7 depend respectively there from). Flowers *et al.* discloses interoperability of network security systems. A vulnerability detection system (VDS) gathers information about a network and processes that information to determine vulnerabilities. The information is gathered and processed based on a set of rules stored in the VDS. An intrusion detection system (IDS) monitors

network traffic for signs of malicious activity based on a set of rules. The rules used by the VDS and IDS are easily formed and therefore an end user can easily define and construct rules beyond any that are defined by the VDS/IDS provider. Each rule is formed based on a set of lexical elements that include a set of statements, a set of templates and a set of reserved words. The templates form the fundamental basis for each rule, defining applications, ports, protocols and actions. Accordingly, intrusion conditions and vulnerability conditions can be defined by rules, which, if true when evaluated based on information gathered by the VDS or IDS, indicate the presence of a particular condition. (*See* col. 2, lines 21-60).

In contrast, applicants' claimed invention discloses a diagnostics engine that provides at least some of the information stored in the lexical rule set(s). Information stored in the lexical rule set(s) can be static (*e.g.,* stored by the diagnostics engine upon initialization) and/or dynamic (*e.g.,* protocol(s) added and/or deleted by the diagnostics engine). For example, the diagnostics engine, upon initialization can store information associated with protocol(s) to be monitored in the lexical rule set(s). Upon determining that a network connectivity problem has potentially occurred (*e.g.,* from the protocol state compressor(s)), the diagnostics engine can store information associated with additional protocol(s) to be monitored in the lexical rule set(s). Similarly, upon determining that a network connectivity problem has been corrected (*e.g.,* by the diagnostics engine and/or externally), the diagnostics engine can delete information associated with selected protocol(s) from the lexical rule set(s). By selectively adding and/or deleting information associated with protocol(s) stored in the lexical rule set(s), the impact of the protocol diagnostic system on a computer system (*e.g.*, client system) can be minimized. (*See* p. 8, lines 17-31).

Flowers *et al.* merely discloses the use of rules formed based on a set of lexical elements that include a set of templates, a set of statements and a set of reserved words. The templates form the fundamental basis for each rule, defining entities such as applications, ports, protocols and actions. Applicants' claimed invention discloses a lexical rule set associated with a protocol state compressor which stores information regarding the structure of subsets of data and protocol specific information. Accordingly, Flowers *et al.* is silent with regard to a protocol diagnostic system comprising a data stream monitor component and a diagnostic engine, where ***the diagnostic engine, upon initialization, stores information associated with protocols to be monitored in the at least one lexical rule set, upon occurrence of a network connectivity problem, stores information associated with additional***

***protocols, and upon correction of the network problem, deletes information associated with selected protocols from the at least one lexical rule set.***

In view of the aforementioned deficiencies of Sheldon *et al.* and Flowers *et al.*, it is respectfully submitted that this rejection be withdrawn with respect to independent claims 1, 4, 19 and 20 (which claims 3 and 7 depend respectively there from).

## II. Rejection of Claim 6 Under 35 U.S.C. §103(a)

In the Final Office Action dated July 5, 2006, claim 6 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Sheldon in view of Flowers *et al.*, and further in view of Bereiter *et al.* (US Patent 6,357,017). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Sheldon *et al.*, Flowers *et al.* and Bereiter *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Bereiter *et al.* does not make up for the aforementioned deficiencies of Sheldon *et al.* and Flowers *et al.* with respect to independent claim 4 (which claim 6 depends from). Thus, the subject invention as recited in claim 6 is not obvious over the combination of Sheldon *et al.*, Flowers *et al.* and Bereiter *et al.*, and withdrawal of this rejection is requested.

## III. Rejection of Claims 8-14 Under 35 U.S.C. §103(a)

In the Final Office Action dated July 5, 2006, claims 8-14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Sheldon in view of Flowers *et al.*, and further in view of Kerft *et al.* (US Patent 5,442,170). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Sheldon *et al.*, Flowers *et al.* and Kerft *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

As stated above, applicants' claimed invention relates to a system and methodology to facilitate network diagnostics and self-healing of network connectivity problem(s). More particularly, independent claim 8 (and similarly independent claim 13) recites a computer network diagnostic system, comprising *a data stream monitor/multiplex component that accesses real-time network data, selectively determines at least one subset of the real-time network data to multiplex based at least in part upon at least one lexical rule set; a data stream distribution engine that demultiplexes the multiplexed data based at least in part upon the at least one lexical rule set; and, a diagnostics engine having a plurality of protocol state compressors, ... ; and where* ***the diagnostic engine, upon***

***initialization, stores information associated with protocols to be monitored in the at least one lexical rule set, upon occurrence of a network connectivity problem, stores information associated with additional protocols, and upon correction of the network problem, deletes information associated with selected protocols from the at least one lexical rule set.*** Sheldon *et al.*, Flowers *et al.* and Kerft *et al.*, individually or in combination, fail to teach or suggest such aspects of the claimed invention.

Sheldon *et al.* relates to a system and method for monitoring and diagnosis of video device performance in the transferring of audio visual data over a video network. A diagnostic node interfaces with a video network to receive audio visual data associated with one or more video devices of the video network. The diagnostic node operates as a transparent pass through/proxy for a video device or as a regular terminating route in order to evaluate audio visual data and determine performance statistics associated with a predetermined video device that is proximate the diagnostic node. (*See* page 1, paragraph [0008]). As stated *supra*, Sheldon *et al.* fails to disclose the use of a lexical rule set for determining subsets of raw network data to copy.

Flowers *et al.* does not cure the deficiencies of Sheldon *et al.* with respect to claims 8 and 13 (which claims 9-12 and 14 depend respectively there from). Flowers *et al.* discloses interoperability of network security systems. A vulnerability detection system (VDS) gathers information about a network and processes that information to determine vulnerabilities. The information is gathered and processed based on a set of rules stored in the VDS. An intrusion detection system (IDS) monitors network traffic for signs of malicious activity based on a set of rules. Each rule is formed based on a set of lexical elements that include a set of statements, a set of templates and a set of reserved words. The templates form the fundamental basis for each rule, defining applications, ports, protocols and actions. (*See* col. 2, lines 21-60). As stated *supra*, Flowers *et al.* does not disclose a diagnostic engine that stores and deletes information associated with selected protocols from the lexical rule set based upon occurrence and correction of a network connectivity problem.

Kerft *et al.* does not make up for the aforementioned deficiencies of Sheldon *et al.* and Flowers *et al.* Kerft *et al.* relates to a programmable cable adaptor that includes a housing containing an internal circuit board having a plurality of conductive traces, an input connector with multiple pins or pin-receiving sockets, and an output connector with multiple pins or pin-receiving sockets. On the circuit board, there is a card edge receptacle with key-contacting pins electrically connected to the conductive traces which in turn electrically couple the receptacle pins to the input connector and/or the output connector. The key-contacting pins of the card edge receptacle are arrayed along at least one

side of an elongated aperture for receiving an adaptor programming key generally referred to as a card edge key. The "key" is typically a small printed circuit board with conductive tabs on at least one side thereof with at least one tab being electrically connected to at least one other tab on the key by conductive traces. When the key is inserted into the receptacle aperture, electrical connections are made between the pins/sockets of the input connector and the pins/sockets of the output connector *via* the tabs and circuit traces on the key. (*See* col. 2, lines 36-57).

Kerft *et al.* is cited by the Examiner to provide a multiplexer. (*See* Final Office Action dated July 5, 2006, p. 7). Accordingly, the combination of Sheldon *et al.*, Flowers *et al.* and Kerft *et al.* does not teach the claimed invention. Specifically, utilizing a multiplexer in a video diagnostic system does not read on the presently claimed diagnostic system, comprising *a data stream monitor/multiplex component that accesses real-time network data and selectively determines at least one subset of the real-time network data to multiplex based in part upon a lexical rule set and a data stream distribution engine that demultiplexes the multiplexed data based in part upon the lexical rule set and, a diagnostics engine having a plurality of protocol state compressors,... ; and where* ***the diagnostic engine, upon initialization, stores information associated with protocols to be monitored in the at least one lexical rule set, upon occurrence of a network connectivity problem, stores information associated with additional protocols, and upon correction of the network problem, deletes information associated with selected protocols from the at least one lexical rule set.***

In view of the aforementioned deficiencies of Sheldon *et al.*, Flowers *et al.* and Kerft *et al.*, it is respectfully submitted that this rejection be withdrawn with respect to independent claims 8 and 13 (which claims 9-12 and 14 depend respectively there from).

## IV. Rejection of Claim 16 Under 35 U.S.C. §103(a)

In the Final Office Action dated July 5, 2006, claim 16 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Sheldon in view of Flowers *et al.*, in view of Kerft *et al.*, and further in view of Korkosz *et al.* (US Patent 6,781,513). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Sheldon *et al.,* Flowers *et al.*, Kerft *et al.* and Korkosz *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Korkosz *et al.* does not make up for the aforementioned deficiencies of Sheldon *et al.*, Flowers *et al.* and Kerft *et al.* with respect to independent claim 13 (which claim 16 depends from). Thus, the subject invention as recited in claim 16 is not obvious over the combination of

Sheldon *et al.,* Flowers *et al.*, Kerft *et al.* and Korkosz *et al.*, and withdrawal of this rejection is requested.

## V. Rejection of Claim 15 Under 35 U.S.C. §103(a)

In the Final Office Action dated July 5, 2006, claim 15 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Sheldon in view of Flowers *et al.*, in view of Kerft et al, and further in view of Korkosz et al, and further in view of Morgan *et al.* (US Patent App. No. 2002/0144187). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Sheldon *et al.,* Flowers *et al.*, Kerft *et al.*, Korkosz *et al.* and Morgan *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Morgan *et al.* does not make up for the aforementioned deficiencies of Sheldon *et al.,* Flowers *et al.*, Kerft *et al.* and Korkosz *et al.* with respect to independent claim 13 (which claim 15 depends from). Thus, the subject invention as recited in claim 15 is not obvious over the combination of Sheldon *et al.,* Flowers *et al.*, Kerft *et al.*, Korkosz *et al.* and Morgan *et al.*, and withdrawal of this rejection is requested.

## VI. Rejection of Claims 17-18 Under 35 U.S.C. §103(a)

In the Final Office Action dated July 5, 2006, claims 17-18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Bereiter *et al.* in view of Morgan *et al.* It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Bereiter *et al.* and Morgan *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

The claimed invention relates to a system and methodology to facilitate network diagnostics and self-healing of network connectivity problem(s). More particularly, independent claim 17 (and similarly independent claim 18) recites a diagnostic engine for a server of a computer system, comprising: *a plain language notification data information store storing plain language notification information associated with a plurality of potential server problems; a protocol specific event information data store storing information associated with server health status;* ***at least one lexical rule set that stores information regarding structure of subsets of data and protocol specific information, where upon occurrence of a network connectivity problem, information associated with additional protocols is stored, and upon correction of the network problem, information associated with the additional protocols is deleted from the at least one lexical rule set****; and a self healing*

*component that analyzes information stored in the protocol specific event information to determine at least one of appropriate corrective action and appropriate plain language notification, the plain language notification based at least in part upon information stored in the plain language notification data store.* Bereiter *et al.* and Morgan *et al.*, individually or in combination, fail to teach or suggest such aspects of the claimed invention.

Bereiter *et al.* discloses a system for providing real-time, interactive technical support and service to personal computer users in a distributed network. A given diagnostic data gathering map is run at the client machine to collect a data set indicative of a current operating state of a machine, a resource associated with the machine, an application or the like. Each map encapsulates a specific set of methods and techniques used to automatically explore the computer system and to gather data. (*See* col. 2, lines 24-52).

In contrast, applicants' claimed invention discloses a diagnostics engine that provides at least some of the information stored in the lexical rule set(s). The diagnostics engine, upon initialization can store information associated with protocol(s) to be monitored in the lexical rule set(s). Upon determining that a network connectivity problem has potentially occurred (*e.g.,* from the protocol state compressor(s)), the diagnostics engine can store information associated with additional protocol(s) to be monitored in the lexical rule set(s). Similarly, upon determining that a network connectivity problem has been corrected (*e.g.,* by the diagnostics engine and/or externally), the diagnostics engine can delete information associated with selected protocol(s) from the lexical rule set(s). By selectively adding and/or deleting information associated with protocol(s) stored in the lexical rule set(s), the impact of the protocol diagnostic system on a computer system (*e.g.*, client system) can be minimized. (*See* p. 8, lines 17-31).

Bereiter *et al.* merely discloses a diagnostic data gathering map run at the client machine to collect a data set indicative of a current operating state of a machine. Bereiter *et al.* does not disclose a diagnostic engine comprising a lexical rule set which stores information regarding the structure of subsets of data and protocol specific information. Accordingly, Bereiter *et al.* is silent with regard to a diagnostic engine, comprising:... ***at least one lexical rule set that stores information regarding structure of subsets of data and protocol specific information, where upon occurrence of a network connectivity problem, information associated with additional protocols is stored, and upon correction of the network problem, information associated with the additional protocols is deleted from the at least one lexical rule set.***

Morgan *et al.* does not cure the deficiencies of Bereiter *et al.* with respect to claims 17 and 18. Morgan *et al.* discloses a diagnostics tool which performs diagnostic functions and provides the results without further user intervention. The tool gathers information from a variety of sources within the system, providing a single point of access for the user. The tool may also be employed as a component in a self-healing system. In this regard, an application error may be sensed and used to trigger the tool. The tool may then provide a result set including diagnostic information, which may then be used by another remedial software component to attempt to rectify any identified problems. The self-healing system may be operated in background or alternatively may provide the user with one or more indications, for example, that a problem has been encountered and diagnostics are being performed, or other status messages providing the user with more information related to identified problems and/or attempted fixes. (*See* p. 1, paragraphs [0009]-[0010]).

As stated *supra*, applicants' claimed invention recites a diagnostic engine comprising a lexical rule set. Morgan *et al.* merely discloses a diagnostic tool that gathers information and provides a result set based on this information. Morgan *et al.* does not disclose a diagnostic engine comprising a lexical rule set which stores information regarding the structure of subsets of data and protocol specific information. Accordingly, Morgan *et al.* is silent with regard to a diagnostic engine, comprising: ... ***at least one lexical rule set that stores information regarding structure of subsets of data and protocol specific information, where upon occurrence of a network connectivity problem, information associated with additional protocols is stored, and upon correction of the network problem, information associated with the additional protocols is deleted from the at least one lexical rule set.***

In view of the aforementioned deficiencies of Bereiter *et al.* and Morgan *et al.*, it is respectfully submitted that this rejection be withdrawn with respect to independent claims 17 and 18.

## CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP300US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731